VG422R

User's Manual

Rev 1.0
2003, 5

CONGRATULATIONS ON YOUR PURCHASE OF VG422R. **1**

THIS PACKAGE CONTAINS 1
CONFIRM THAT YOU MEET INSTALLATION REQUIREMENTS 1

1. INSTALLATION GUIDE 2

1.1. HARDWARE SETUP 2
1.1.1. VG422R – Front Panel 2
1.1.2. VG422R – Rear Panel 3

2. DEFAULT VALUES 4

2.1. PASSWORD 4
2.2. DEFAULT NETWORK SETUP 4
2.3. DEFAULT VOIP SETUP 4
2.4. OTHER DEFAULT SETUP 4

3. CONFIGURING YOUR VG422R – LOGIN 5

4. CONFIGURING YOUR VG422R – GENERAL SETUP 6

4.1. SYSTEM 6
4.1.1. Time Zone 6
4.1.2. Password Settings 6
4.1.3. Remote Management 6
4.2. VOIP SETTINGS 7
4.2.1. Dial Setting 7
4.2.2. Port Setting 8
4.2.3. Outgoing Mode 9
4.2.4. H.323 Setting 10
4.2.5. PBX ID / Prefix Setting for Incoming 11
4.2.6. Peer Gateway 12
4.2.7. User Management 12
4.3. WAN SETTINGS 12
4.3.1. Dynamic IP 12
4.3.2. PPPoE 13
4.3.3. Static IP 13
4.3.4. PPTP 14
4.4. LAN SETTINGS 14
4.5. NAT SETTINGS 15
4.5.1. Address Mapping 15
4.5.2. Virtual Server 15
4.5.3. Special Application 16
4.6. FIREWALL 17
4.6.1. Access Control 17
4.6.2. URL Blocking 19
4.6.3. Schedule Rule 19
4.6.4. Intrusion Detection 21
4.6.5. DMZ 22

5. UPNP 23

6. DYNAMIC DNS 23

7. TOOLS 23

7.1. CONFIGURATION TOOLS 23
7.2. FIRMWARE UPGRADE 24
7.3. RESET 24
8. STATUS 24
8.1. INTERNET CONNECTION 25
8.2. DEVICE STATUS 25
8.3. SECURITY LOG 25
8.4. DHCP CLIENT LOG 26
8.5. VOIP STATUS 26

Congratulations on your purchase of VG422R.

VG422R is a broadband router designed to share Internet Access, provide security, and to network multiple devices for a variety of users. The VG422R's simple installation setup can be used by the least experienced of users, while providing networking professionals with easy to configure advanced features. Please read the User Guide for advanced features of this product.

This Package Contains

- One VG422R
- One Power Adapter
- One User Manual CD
- One Category 5 Fast Ethernet Cable

Confirm That You Meet Installation Requirements

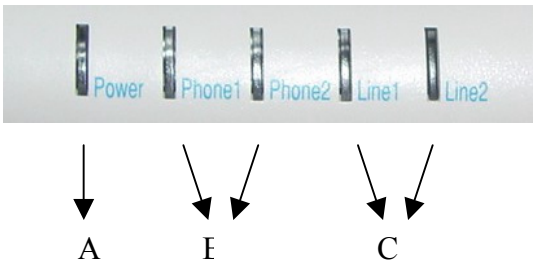
Before proceeding with the installation of your VG422R, please be sure you have the following:

- A computer with an Ethernet network card installed.
- Your Windows CD, if your computer is running Windows 95, 98, ME, 2000 or XP.
- An Internet connection through a cable or DSL modem or an external dial-up or ISDN modem.
- An additional Ethernet network cable.
- A Web browser such as Internet Explorer or Netscape.

1. Installation Guide

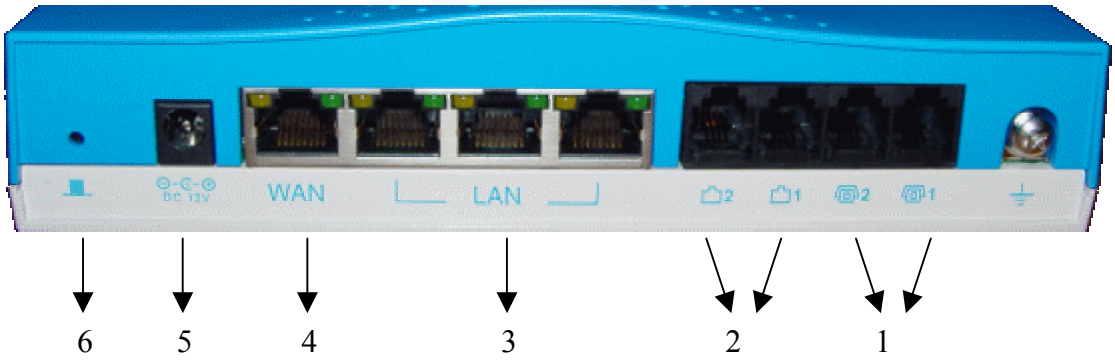
1.1. Hardware Setup

1.1.1. VG422R – Front Panel



Item	LED	Color	Condition	Status
A	Power	Green	On	Device is receiving power.
B	Phone1 Phone2	Orange	On	Off hook Phone set
			Flashing	Phone port is receiving ring.
C	Line1 Line2	Orange	On	Off hook Line port incoming call
			Flashing	Line port is receiving ring.

1.1.2. VG422R – Rear Panel



Item	Connector	Function
1	**Phone1** **Phone2**	Connect to Phone set。(Or Connect to PBX CO Line)
2	**Line1** **Line2**	Connect to PSTN Line。
3	**Local (1-3)**	3 port (10/100Mbps) RJ-45 connector, connect to PC or local switch/hub.
4	**WAN**	Connect to Cable or ADSL Modem 。
5	**12V DC**	Power connector.
6	**RESET** **(Reboot)**	Reset button. Press for one **second** to reset the device or press for 5 seconds to reset to the factory default.

1. Connecting Phone set: Connect phone set directly to VG422R on phone1-2.
2. Connecting PSTN Line: Connect PSTN line directly to VG422R on Line1-2.
3. Connecting Computers: Connect computers directly to VG422R on ports 1-3 of the LAN ports. If you have more than 3 computers to plug in, connect a hub or a switch (using its uplink port) and connect additional computers to that device**.**
4. Connecting a Cable Modem or DSL Modem: Connect your Cable or DSL modem to the WAN port on the rear panel.
5. Power: Plug the power cord into the power jack.
6. The device will boot up at this moment. Make sure the LED in front panel light up correctly.

2. Default Values

2.1. Password

The default user name / password is root / root. For security and management reason, we suggest you to set up a password after first login to the system. If you forget the user name / password, you can push the reset button for more than 5 seconds, until all the LEDs flash, your VG422R will be reset to factory default.

2.2. Default Network setup

LAN Setup		WAN Setup
IP Address	192.168.1.1	DHCP Client enabled
Subnet Mask	255.255.255.0	
DHCP server	Enable	
DHCP IP range	100 IP addressed from 192.168.1.100 to 192.168.1.199	

2.3. Default VoIP setup

International call prefix	002
Long distance call prefix	0
Country code	886
Area code	2(Taipei)
Phone 1 number	1011
Phone 2 number	1012
Line mode	Dedicated Line mode

2.4. Other Default setup

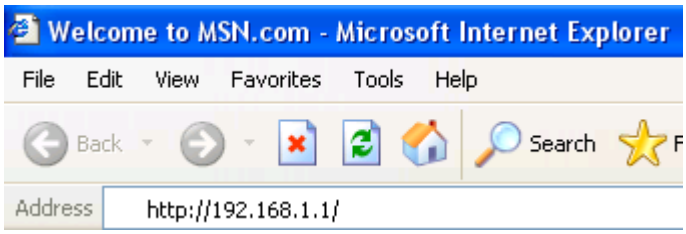
Time Zone	Taipei
Firewall	Off
WAN	DHCP
UPnP	Off
DDNS	Off

3. Configuring Your VG422R – Login

Now that you have successfully configured your computer and retrieved your new network settings from your VG422R, you are ready to configure the VG422R's settings for your LAN.

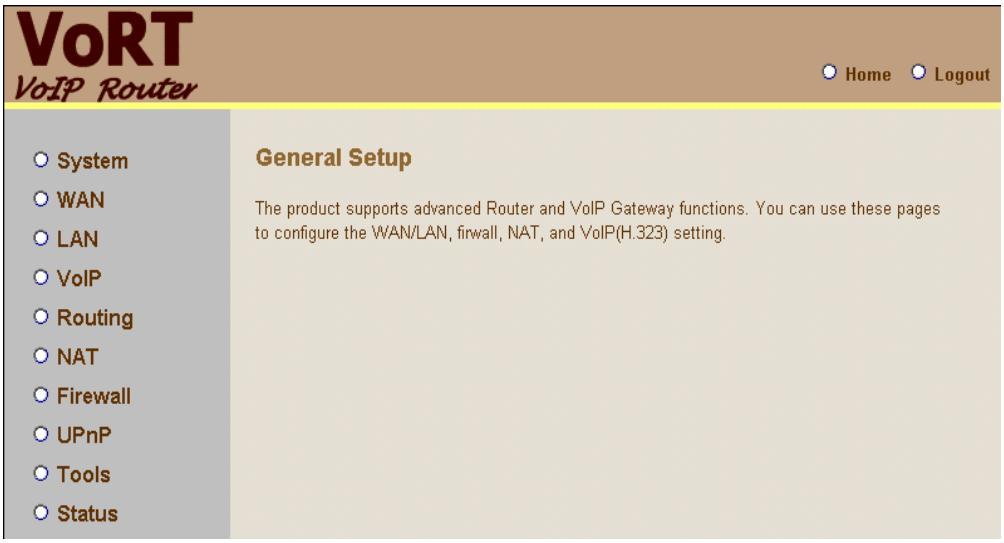
1. Open your Web browser (i.e., Internet Explorer or Netscape Navigator) and click the stop button.

2. In the "Address" field type "http://192.168.1.1/" and press <ENTER>.



3. The VG422R login screen will appear. Leave the Password field empty and click on "login". The default Username/Password setting is "root/root". For security reasons, you should assign a password as soon as possible. Note that the password login in case sensitive.

4. Once the user login successfully, the first page will appear as below:

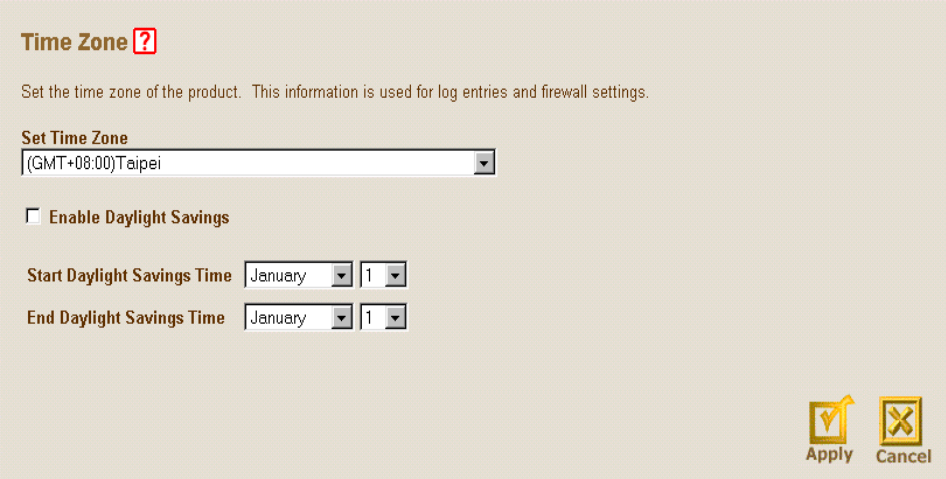


4. Configuring Your VG422R – General Setup

4.1. System

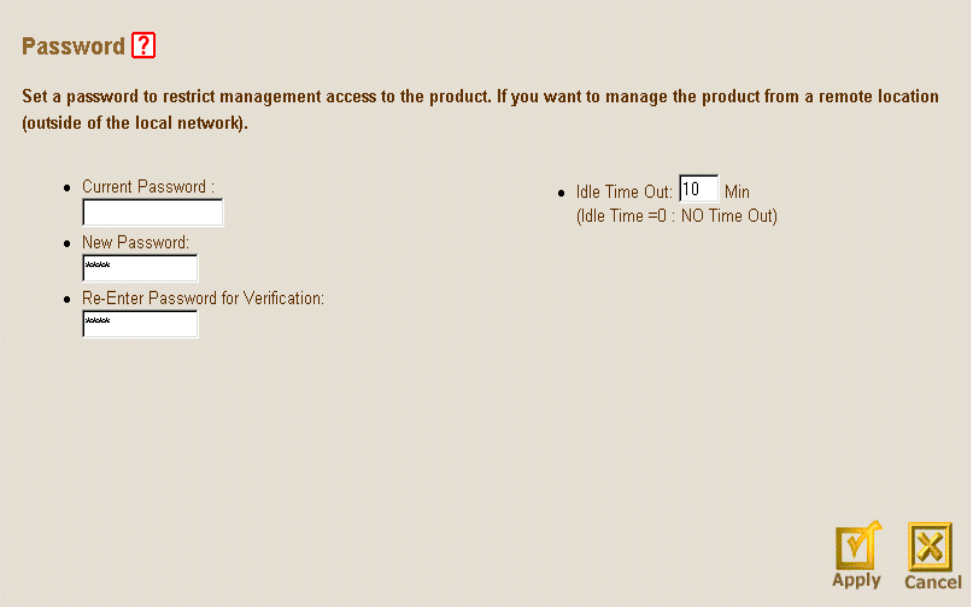
4.1.1. Time Zone

Set the proper time zone and the daylight savings for VG422R.



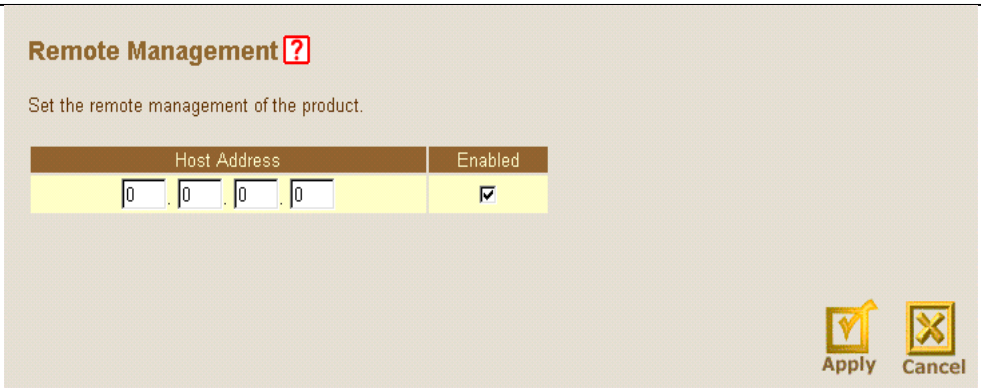
4.1.2. Password Settings

Set the password of the user. The Idle Time Out value is used for VG422R to log out automatically when no access to the web after this timeout value.

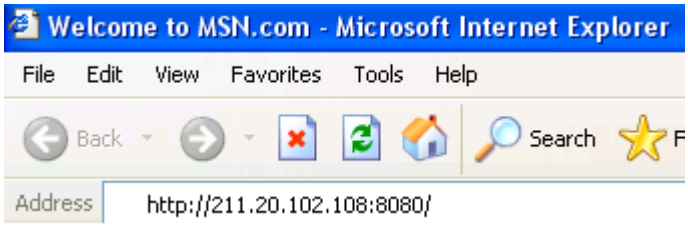


4.1.3. Remote Management

The "Remote Management" feature can restrict remote user login from the WAN port. The IP setting of "0.0.0.0" allows user from any IP address to remote logged in to the device. When the 'Enabled" is not checked, remote login is disabled.



The remote user can login using WAN IP. The default port number is 8080.

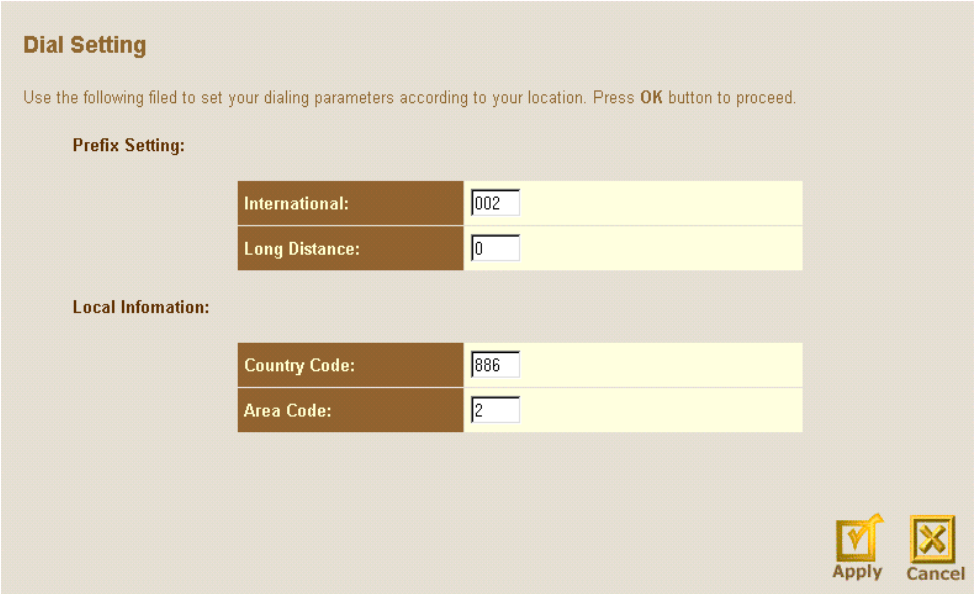


4.2. VoIP Settings

The VG422R provide Dial setting and Port setting for VoIP user.

4.2.1. Dial Setting

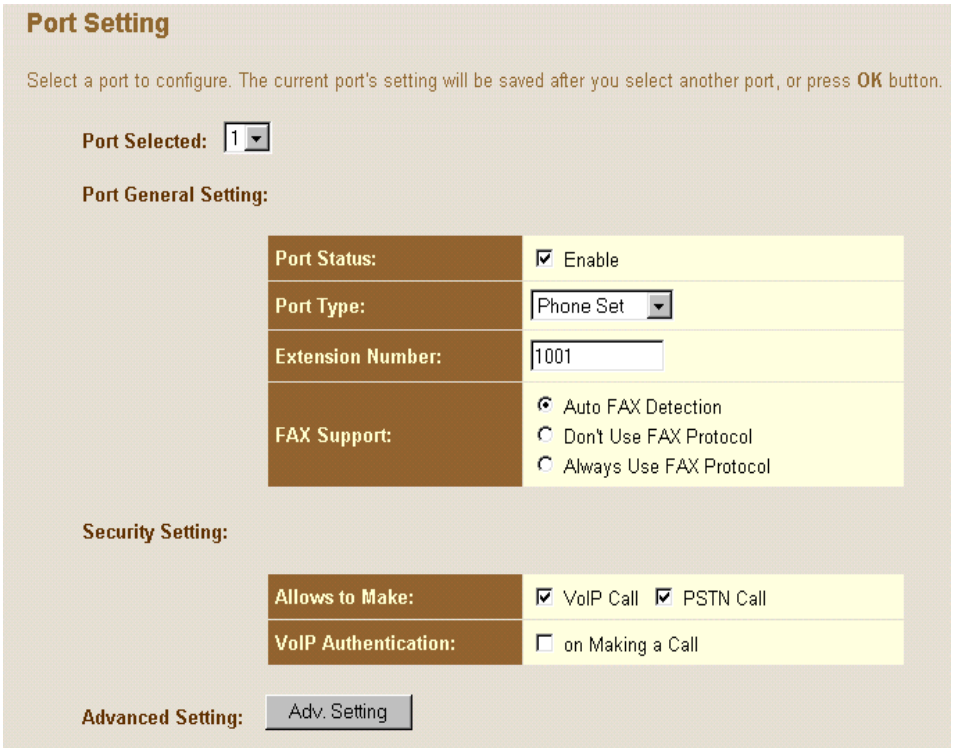
This page sets up the parameters related to the prefix of the phone numbers, including International call prefix, Long distance call prefix, country code and area code.



4.2.2. Port Setting

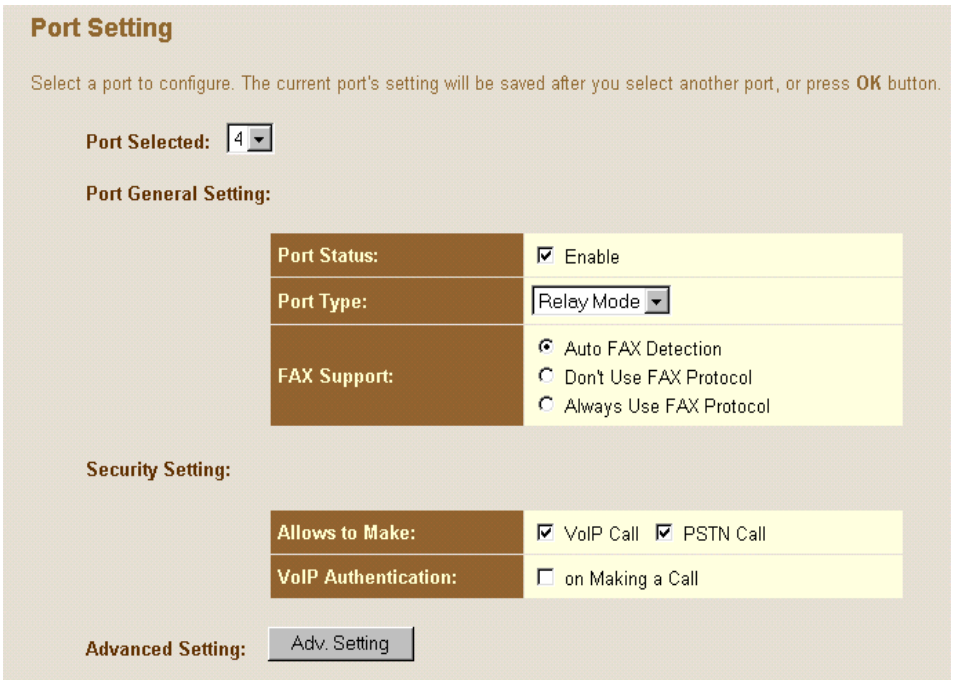
This page defines the general port parameters and user must select port number first.

In the port1 and port2, we have Web Page as following. The default setting is Phone Set and extension number is 1011/1012. But the real extension number will get from Service Center.



In the port3 and port4, we have Web Page as following. The default setting is Relay mode.

Port3 will relay to port1 and Port4 will relay to port2.

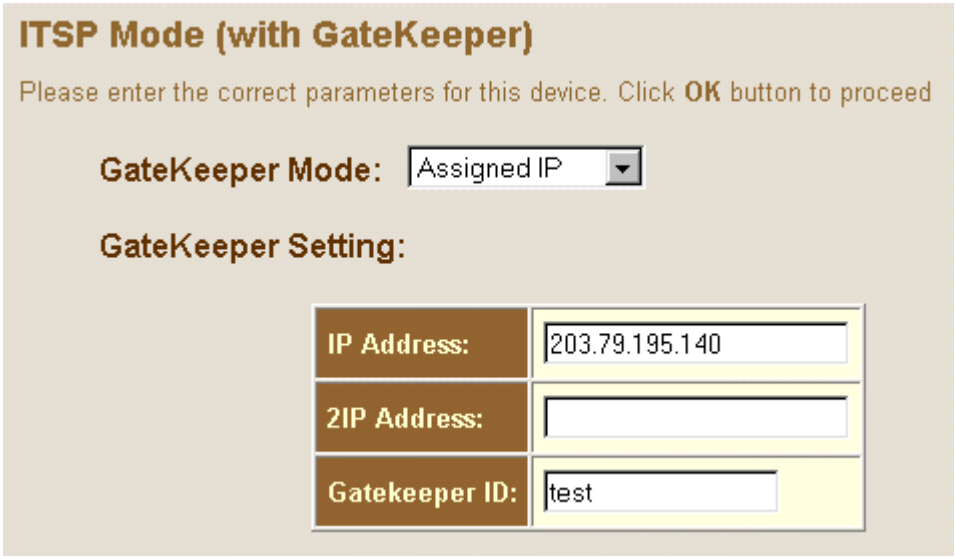


If you enable VoIP authentication, any incoming call will invoke IVR to guide you input user id and password. The user id and password is entered in user management.

4.2.3. Outgoing Mode

In the outgoing mode, we provide Enterprise and ITSP mode to find out peer gateway IP address.

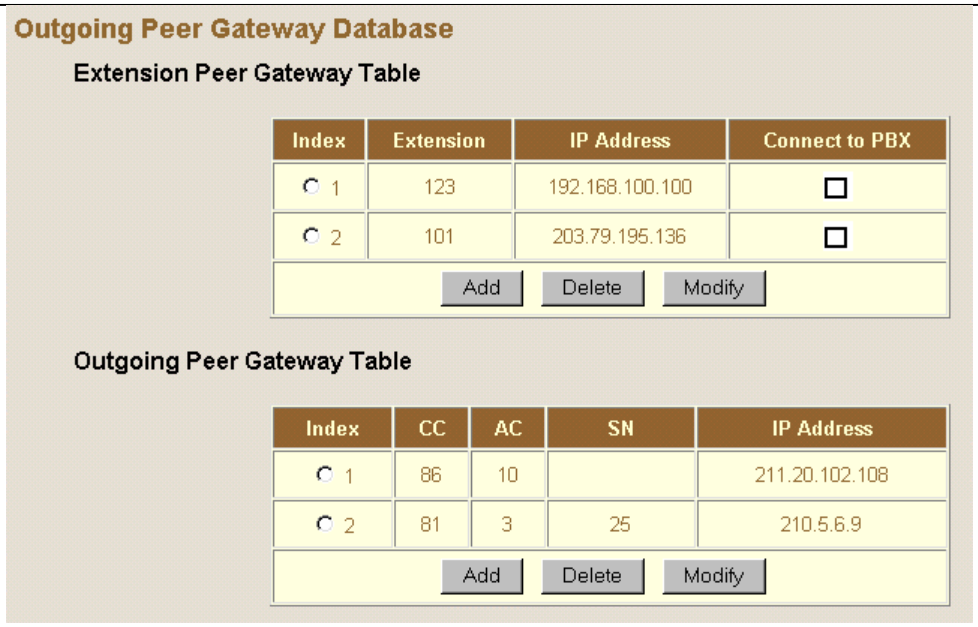
In most case, we use ITSP mode to find peer gateway. The ITSP system provide gatekeeper to control all of VoIP gateway. Every gateway login gatekeeper and provide basic information to gatekeeper including port extension number and IP address. So, ITSP mode can support dynamic IP users like DHCP, PPPoE and PPTP users.



The system administrator must enter gatekeeper IP. If the default gatekeeper is not able to normally operate. The gateway system will automatically login to 2nd gatekeeper.

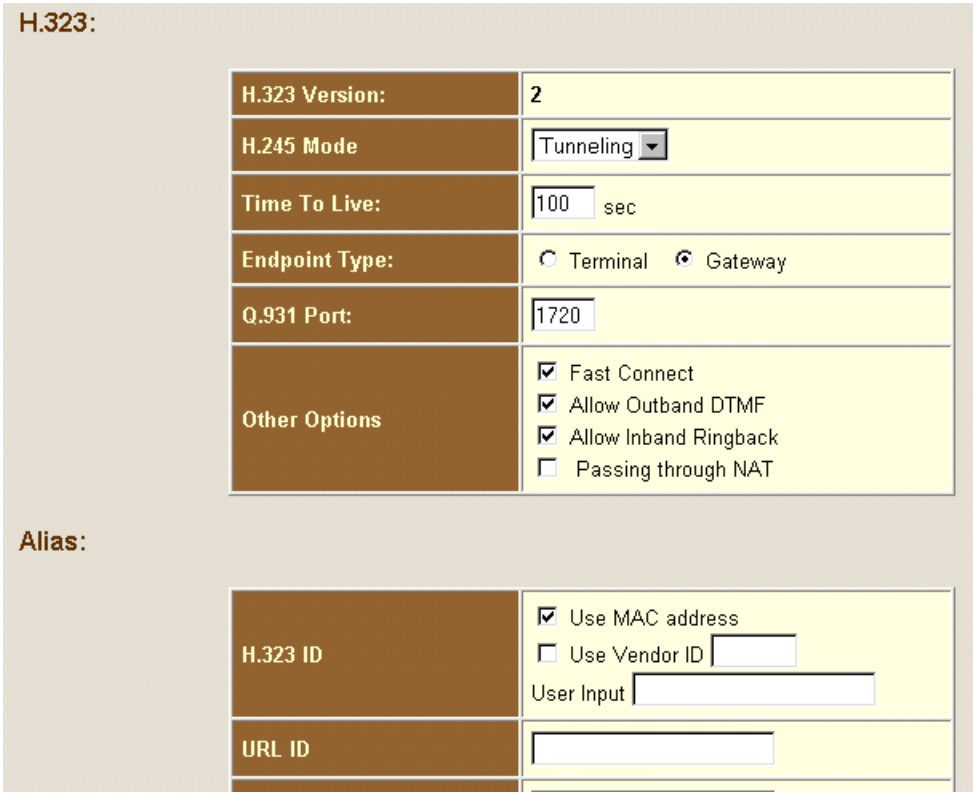
In the enterprise mode, we should define outgoing peer gateway information by extension or prefix.

For example, you dial *123#, system will search extension table, and return IP to you. And if you dial 002-86-10-xxxxxxxx, after E.164 processing, you will get 86-10- xxxxxxxx, then they will meet 8643 prefix in prefix table, and return IP to you. So you cannot use any dynamic IP in this mode.



4.2.4. H.323 Setting

We provide H.323 related setting in this page. If you have any interoperability problem, you must change some setting in this page.

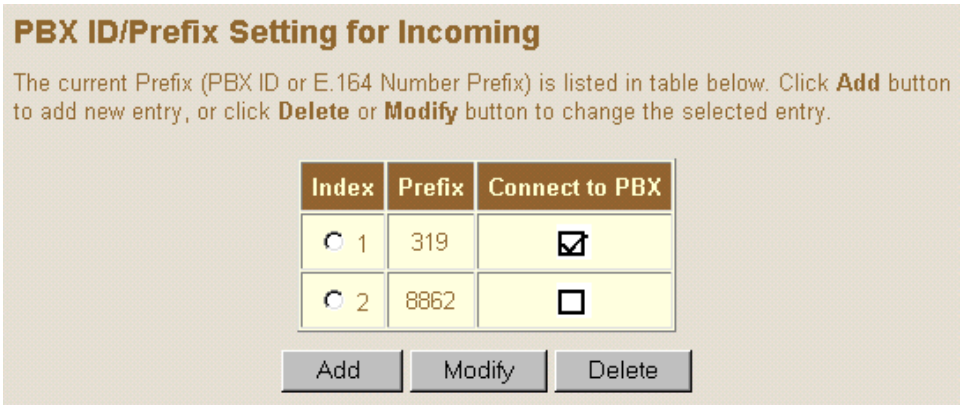


We use the MAC address as H.323 ID. Sometimes ITSP will ask you to change H.323 ID, then you should disable “use MAC address” and enter your H.323 ID in user input field.

4.2.5. PBX ID / Prefix Setting for Incoming

If you set port type to be PBX CO line, you should set PBX ID here. For example, you set port1 and port2 to be PBX CO line, and set PBX ID 319 in this page. The port1 and port2 use 319 as their number. If port1 is busy, system will ring port2. They use same PBX ID number as their number.

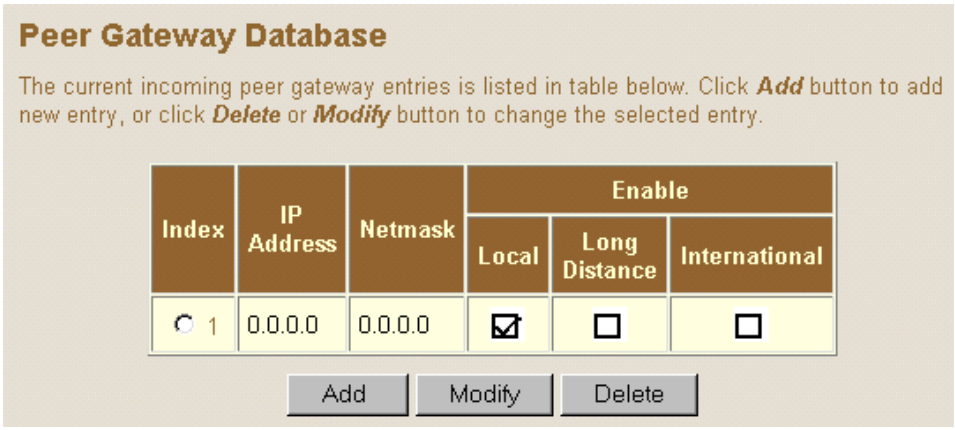
If you set port type to be 'dedicated line', and you want to make this port accept call from Internet. You should set prefix. For example, you set port3 to be 'dedicated line' and set 8862 as prefix, this port will accept call from Internet for any 8862 prefix number call.



4.2.6. Peer Gateway

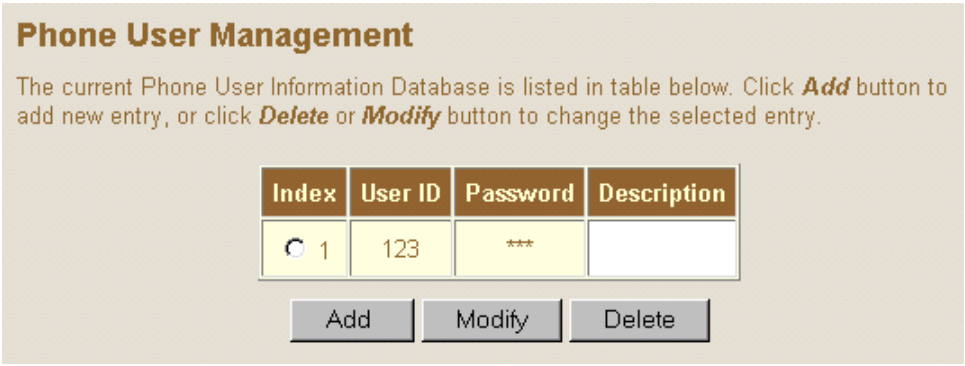
You can define any peer gateway in this table. First you may list any peer gateway by IP and net mask, then you can set call out limitation for that peer gateway, for example Local only, or Long distance or International call.

But 0.0.0.0 means no more peer gateway limitation. Any VoIP call can be accept by this gateway.



4.2.7. User Management

If you enable VoIP authentication, any incoming call will invoke IVR to guide you input user id and password. Where can I set user id and password? The answer is User management. You can set user id and password here. But that is number digit only.

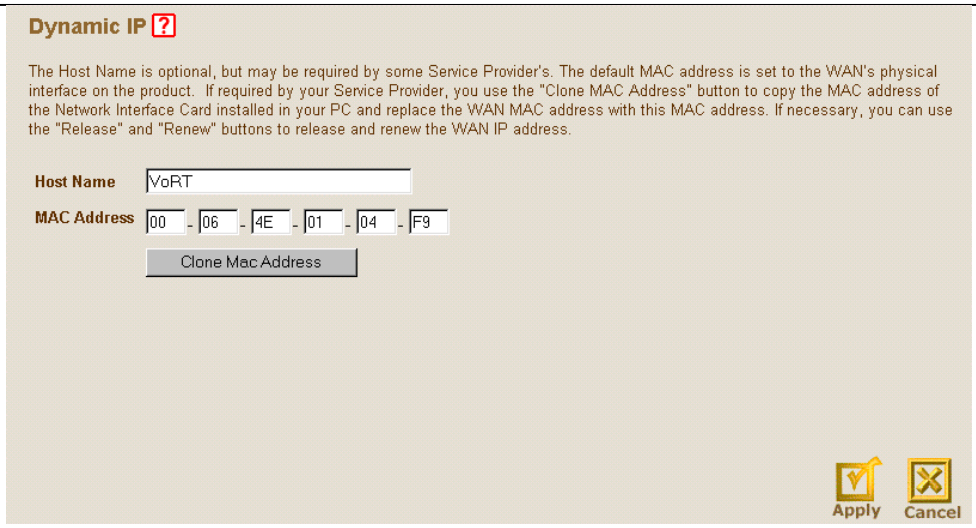


4.3. WAN Settings

The VG422R supports 4 types of WAN connection – Dynamic IP (DHCP Client), PPPoE, Static IP and PPTP.

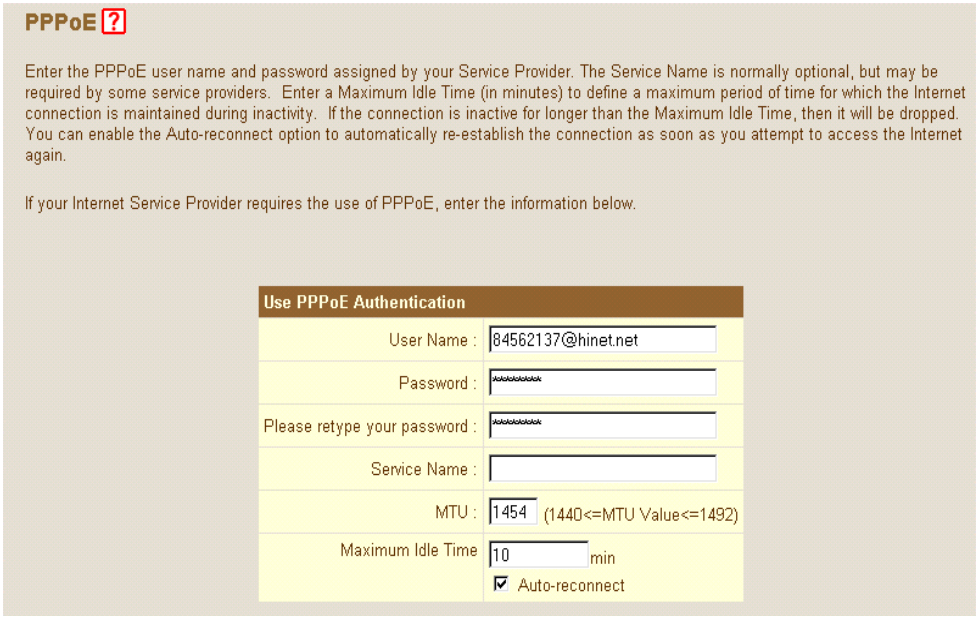
4.3.1. Dynamic IP

Under this mode, VG422R enables DHCP client to get IP address automatically from your service provider. The Host Name is optional, but may be required by some Service Provider's. The default MAC address is set to the WAN's physical interface on the VG422R. If required by Service Provider, you use the <Clone MAC Address> button to copy the MAC address of the Network Interface Card installed in your PC and replace the WAN MAC address with this MAC address. If necessary, you can use the <Restore> buttons to restore the WAN IP address.



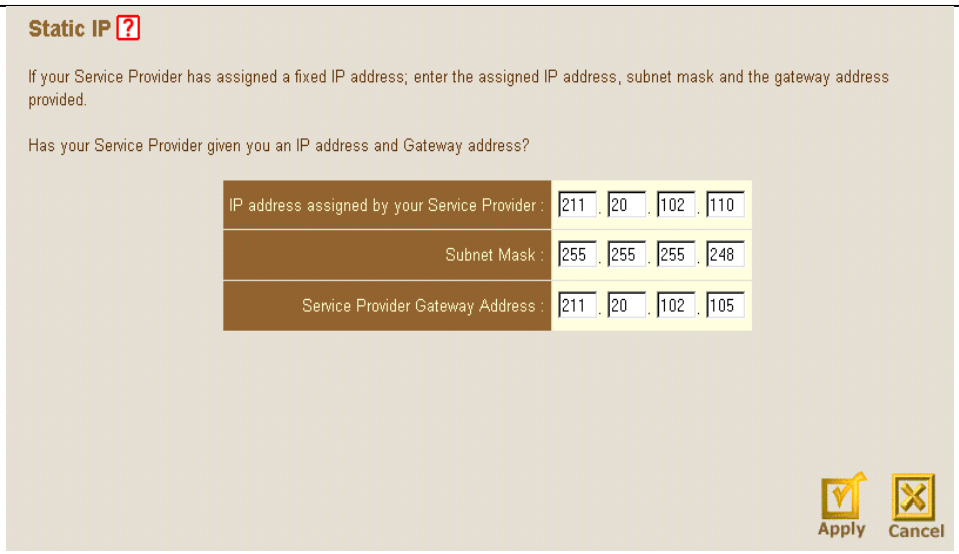
4.3.2. PPPoE

Under this mode, VG422R is acting as a PPPoE client. Enter the PPPoE user name and password assigned by your Service Provider. The Service Name is normally optional, but may be required by some service providers. Enter a Maximum Idle Time (in seconds) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped. You can enable the Auto-reconnect option to automatically re-establish the connection as soon as you attempt to access the Internet again



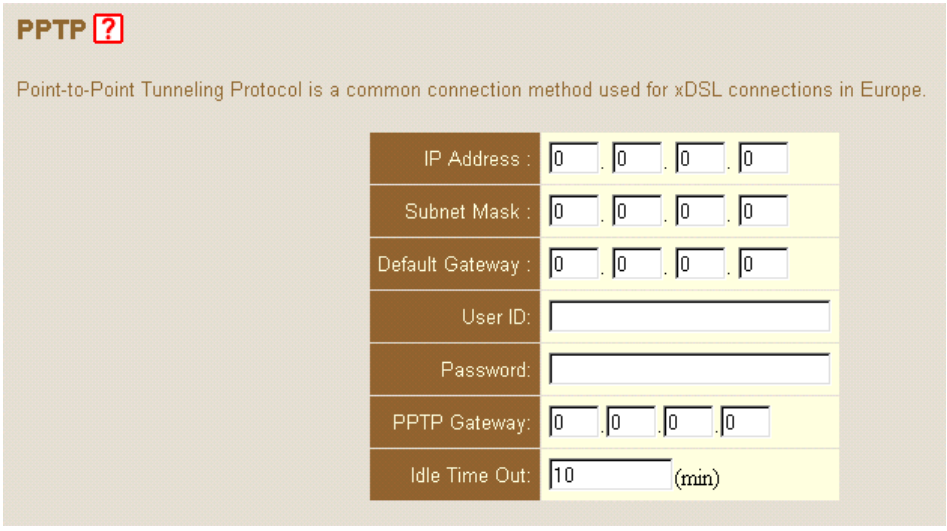
4.3.3. Static IP

If your Service Provider has assigned a fixed IP address, enter the assigned IP address, subnet mask and the gateway address provided. Most service providers provide a DNS server for speed and convenience. If there is a DNS server that you would rather use, you need to specify the IP address here.



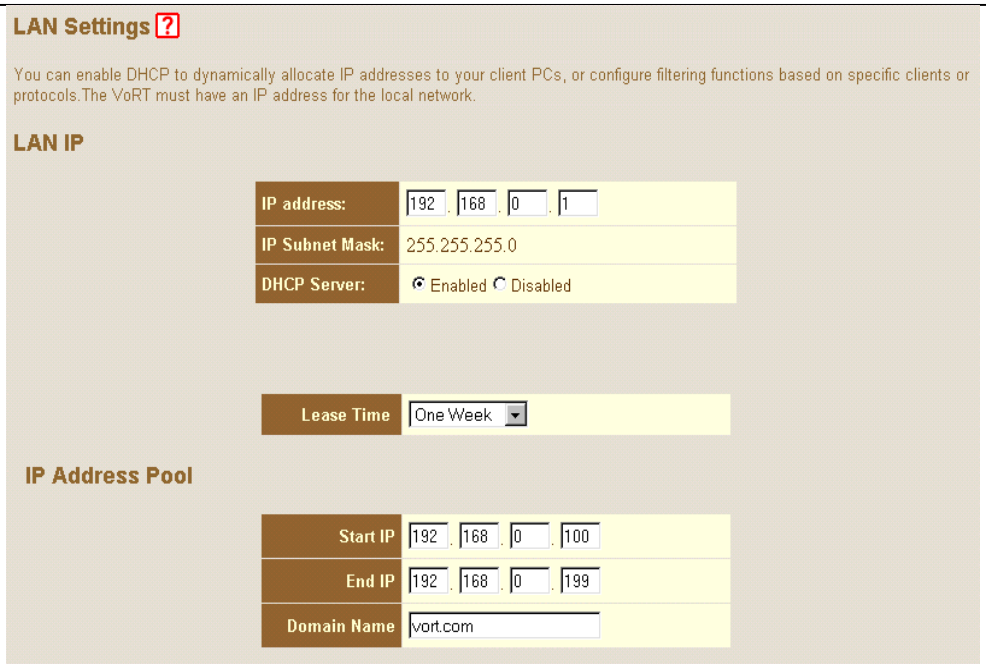
4.3.4. PPTP

Under this mode, VG422R-SIP is acting as a PPTP client. Enter the PPTP IP Address, Subnet Mask, Default Gateway, User ID, Password and PPTP Gateway assigned by your Service Provider. Enter a Maximum Idle Time (in seconds) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the Maximum Idle Time, then it will be dropped.



4.4. LAN Settings

VG422R needs to have an IP address of the local network. You can enable DHCP to dynamically allocate IP addresses to your client PCs. When DHCP server is enabled, you need to enter the IP address range for the local hosts.



4.5. NAT Settings

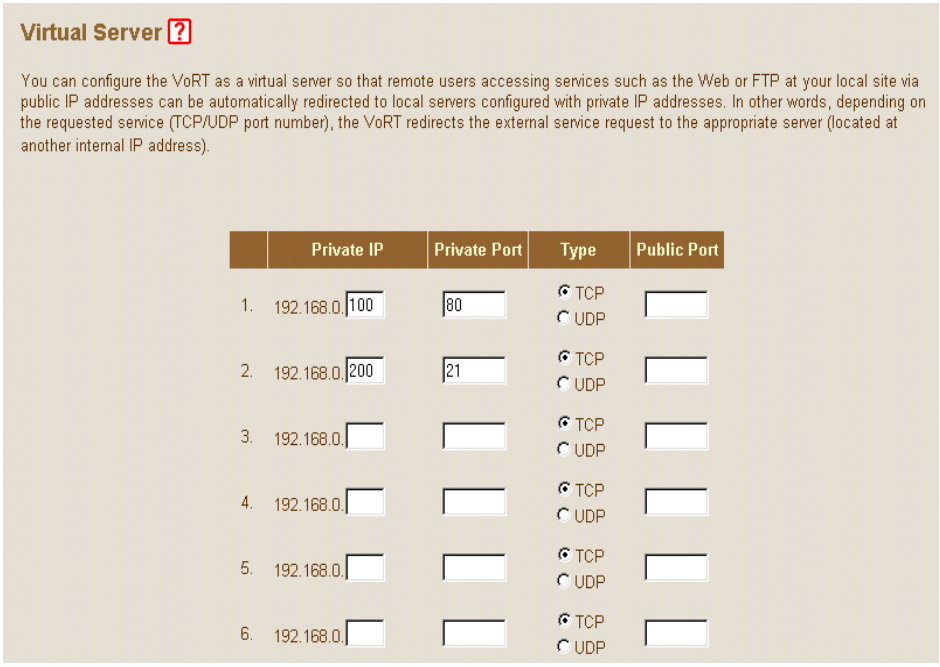
4.5.1. Address Mapping

VG422R supports multiple global IP addresses. It allows IP addresses used in a private local network to be mapped to one or more addresses used in the public, global Internet. This page allows user to enter up to 10 addresses mapping between a set of private IP addresses and one global IP address. After setting, VG422R will map the set of private IP addresses to the global IP address when accessing to the Internet. This is very useful in the gaming and some particular multimedia applications.

4.5.2. Virtual Server

VG422R is a NAT router. All the IP addresses coming in and going out to VG422R can be converted between public and private IP addresses. You can configure VG422R as a virtual server so that remote users accessing services such as the Web or FTP at your local sites via public IP address can be automatically redirected to local servers configured with private IP address. In other words, depending

on the requested service (TCP/UDP), the VG422R redirects the external service request to the appropriate server.

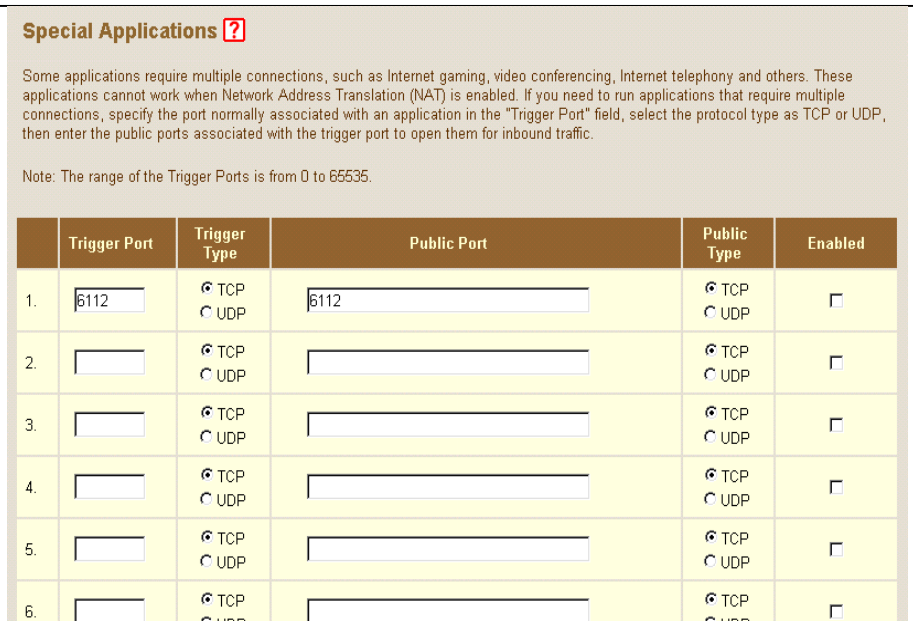


Some of the popular applications and protocol/port numbers mapping are defined below:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

4.5.3. Special Application

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications cannot work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.



Some of the applications are listed below:

Example:

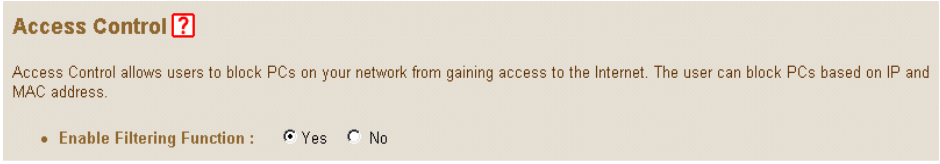
ID	Trigger Port	Trigger Type	Public Port	Public Type	Comment
1	28800	UDP	2300-2400, 47624, 28800	UDP	MSN Game Zone
2	28800	UDP	2300-2400, 47624, 28800	TCP	MSN Game Zone
3	6112	UDP	6112	UDP	Battle.net

4.6. Firewall

VG422R provides extensive firewall protection by restricting connection parameters to limit the risk of hacker attack, and defending against a wide array of common attacks. When firewall is enabled, extra checking will be performed for each packets passing through the device, the performance of the device will be greatly affected. To enable the firewall feature, select <Enable> from firewall page:

4.6.1. Access Control

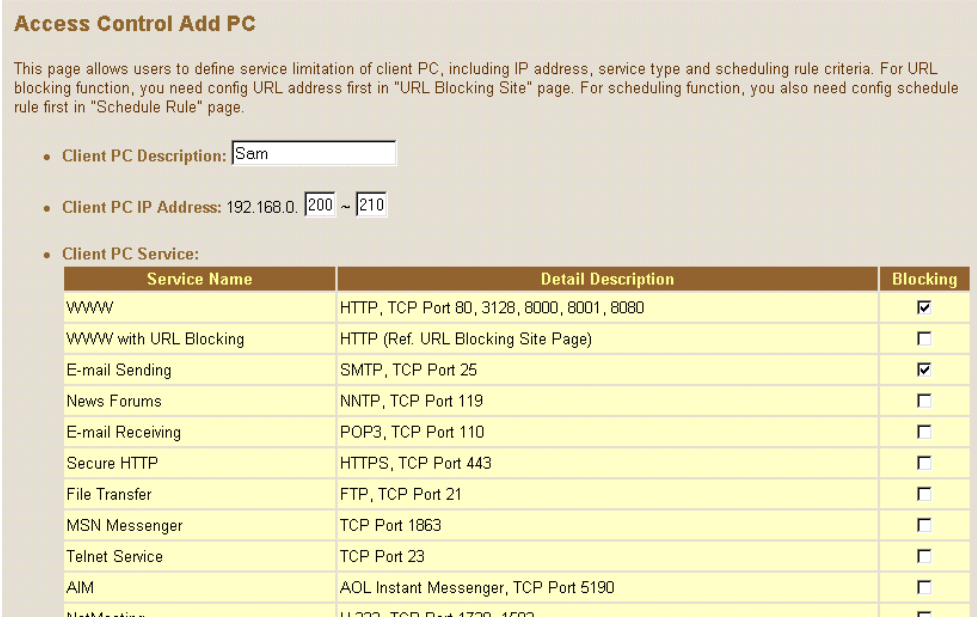
Access Control allows users to block PCs on your network from gaining access to the Internet. The user can block PCs based on IP and MAC address. When firewall is enabled, Access Control will be enabled automatically. User can disable filtering feature manually. When Access Control is enabled, all the packets will be allowed by default, user can use <Normal Filtering Table> and <MAC Filtering Table> to filter out un-allowed traffic.



Normal Filtering Table

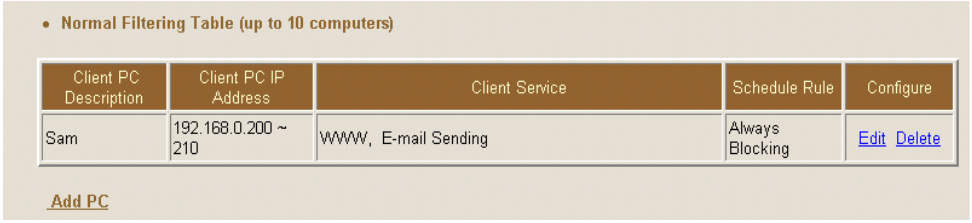
User can press <Add PC> to edit packet-filtering rules.

When user selects <Add PC>, the following <Access Control Add PC> page will show up:



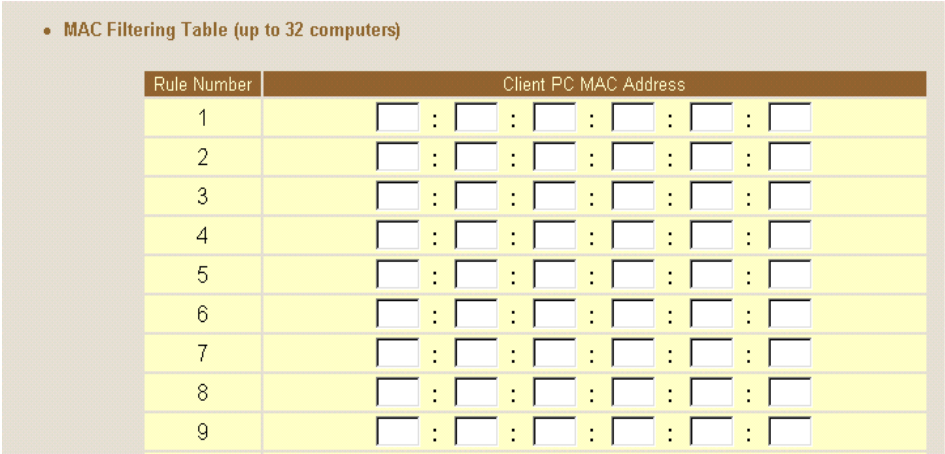
This page allows users to define service limitation of client PC, including IP address, service type and scheduling rule criteria. For URL blocking function, you need configure URL address first in "URL Blocking Site" page. For scheduling function, you also need configure schedule rule first in "Schedule Rule" page.

As shown above, user enter Client PC Description (Sam), and it's IP address (192.168.2.100), and select service name <WWW> and <E-mail Sending>, and press <OK>. The follow page will show up. After the setup, the PCs with IP address from 192.168.2.200 to 192.168.0.210 will not be able to use WWW and sending e-mail. VG422R supports up to 32 filtering rules.



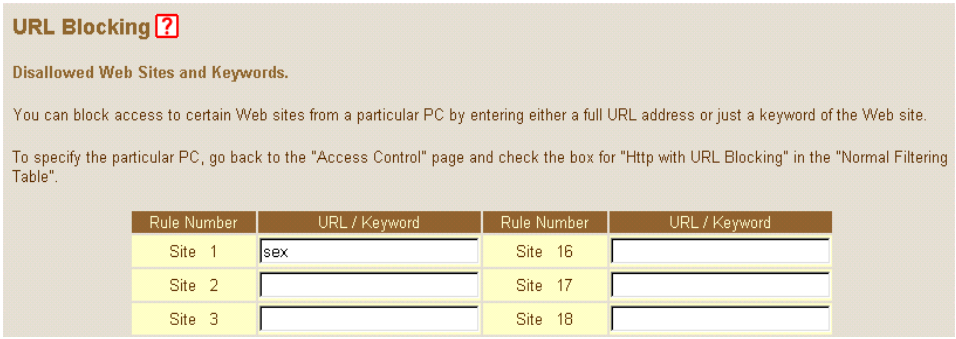
MAC Filtering Table

User can enter up to 32 MAC addresses; the PCs with these MAC addresses will not be allowed to access Internet.



4.6.2. URL Blocking

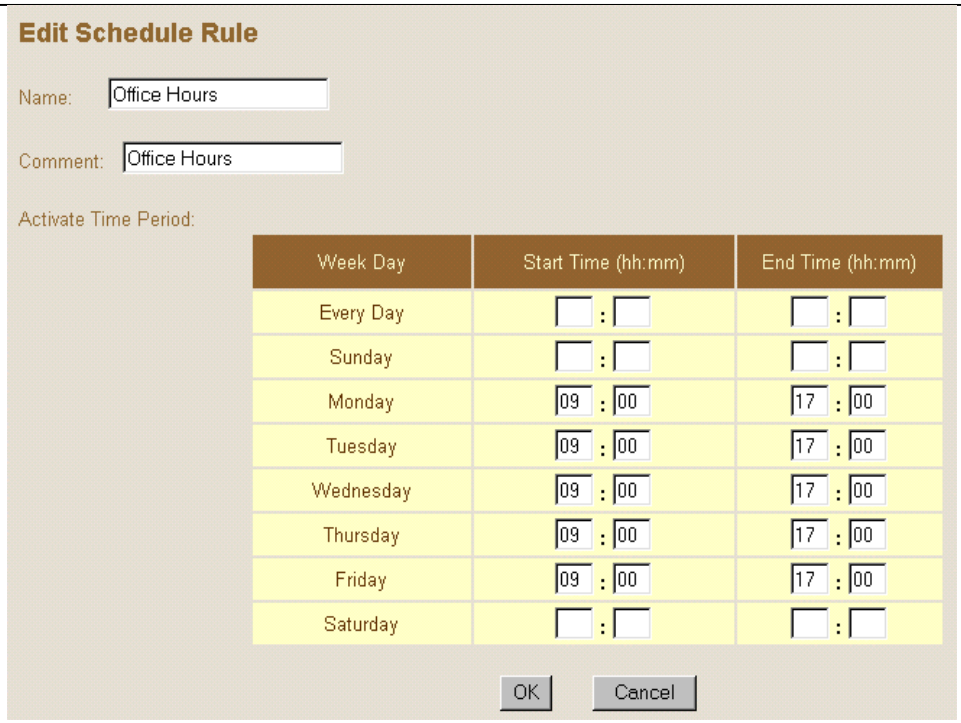
You can block access to certain Web sites from a particular PC by entering either a full URL address or just a keyword of the Web site.
To specify the particular PC, go back to the "Access Control" page and check the box for "Http with URL Blocking" in the "Normal Filtering Table".



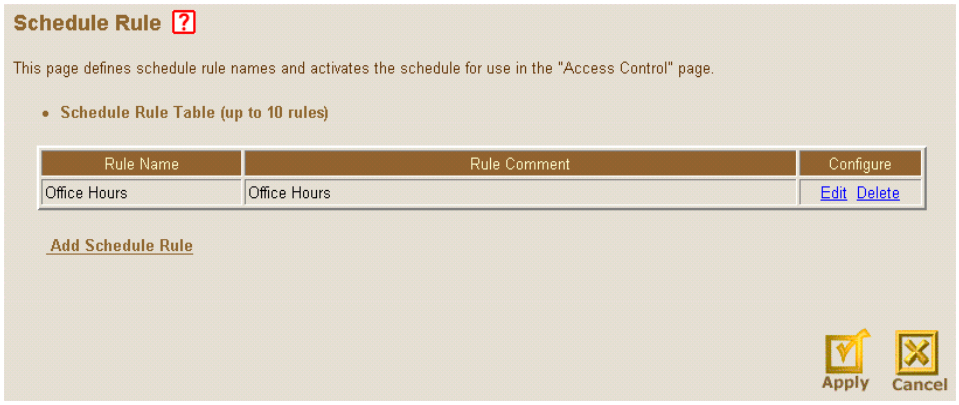
As shown above, all the URLs with ”sex” can not be accessed. The users within LAN cannot access to any web site with “sex” in its URL address.

4.6.3. Schedule Rule

This page allows user to define schedule rule for use in <Access Control> page. User press <Add Schedule Rule> to add schedule name and effective time period. This defined schedule rule will be used under <Access Control Add PC>.

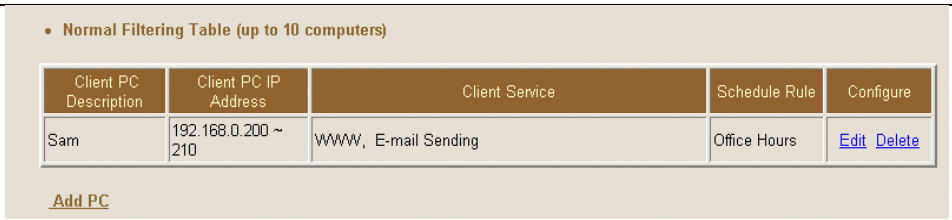


As shown above, we defined a schedule rule called "Office Hour"; the active time period is Monday to Friday, 9:00 am to 5:00 pm. After pressing <OK>, the following page will show up.



Then when we go to <Access Control> page, select <Add PC>, in the bottom of the page <Access Control Add PC>, the scheduling rule will show "Office Hour", as shown below.

If we setup the PC of finance department in our company (IP address 192.168.0.200 to 192.168.0.210) can not access Web during office hour, then in <Access Control> page, we will see the following page.



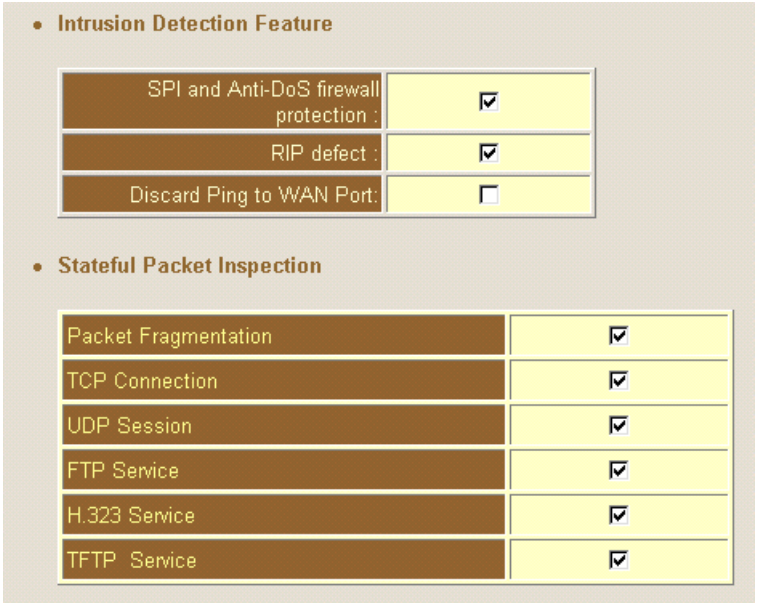
4.6.4. Intrusion Detection

When the SPI (Stateful Packet Inspection) firewall feature is enabled, all packets can be blocked. Stateful Packet Inspection (SPI) allows full support of different application types that are using dynamic port numbers. For the applications checked in the list below, the product will support full operation as initiated from the local LAN.

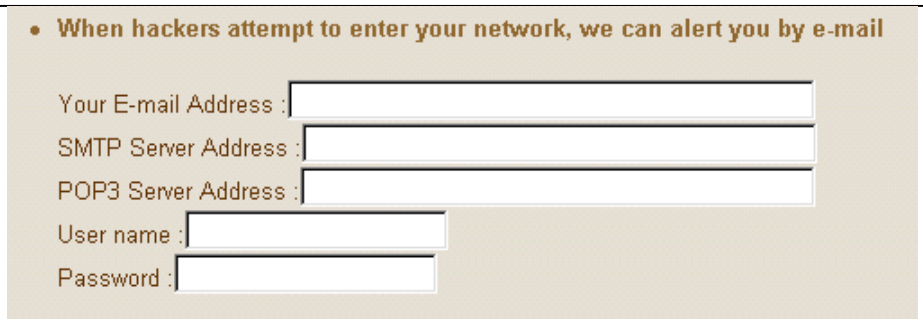
The product's firewall can block common hacker attacks, including IP Spoofing, IP with zero length, IP With Option, Too Short ICMP, Too Short TCP, Too Short UDP, Tiny Fragment Attack, NewTear Attack, Smurf Attack, Land Attack, Ping of Death, UDP Loop Attack, Tear Drop Attack, Snork Attack, Winnuke Attack, Bonk Attack, ASCEND Probe Attack, Boink Attack, SYN Drop Attack, Empty Fragment Attack, Oshare Attack, TCP null scan, TCP Xmas scan, RIP defect, ICMP defect, TCP SYN flood, UDP flood 及 Fragmentation Flood。

Intrusion Detection Features:

SPI and Anti-DoS Firewall Protection	Activate SPI and Anti-DoS protection
RIP Defect	Reject the RIP packets from WAN
Discard PING from WAN	Reject all the PING request to the WAN port

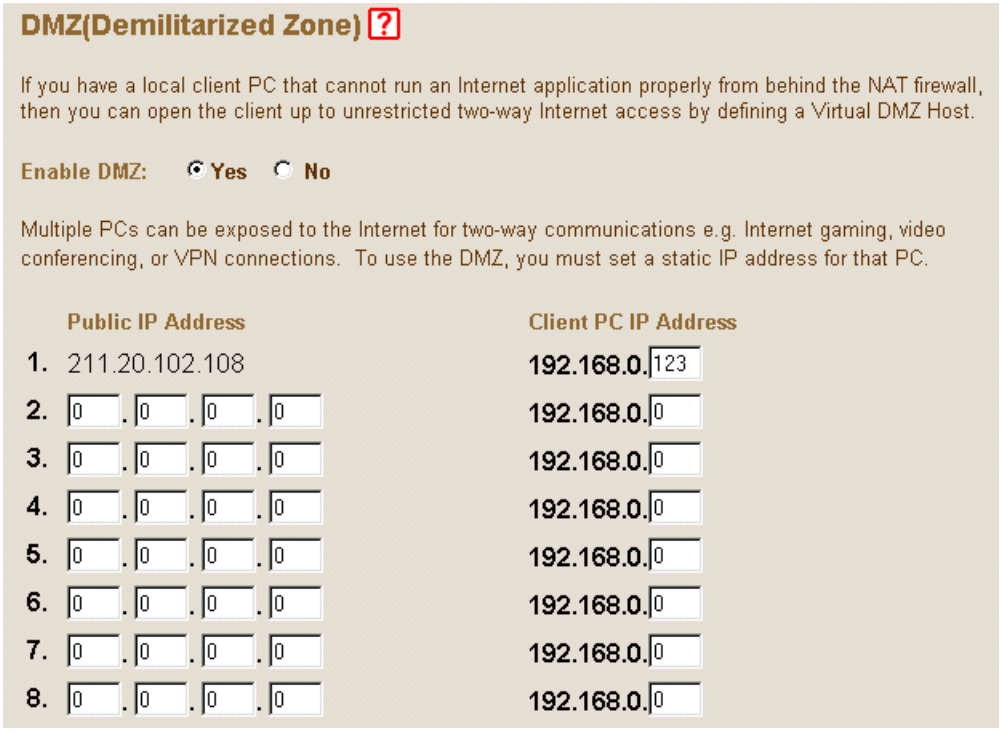


When hacker tries to attack, VG422R can send e-mail alert to the specified user. Enter related e-mail information such as e-mail address and SMTP server. Some e-mail service providers require user to enter POP3 information when trying to send e-mail. In this case, enter the POP3 server, user name and password; otherwise, you don't need to enter POP3 related information.



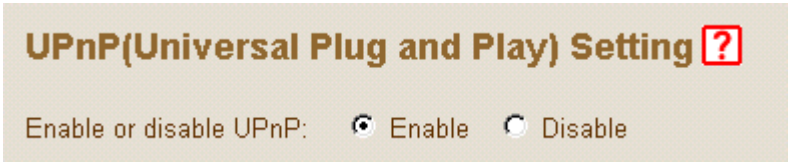
4.6.5. DMZ

A DeMilitarized Zone (DMZ) is a network off one of the LAN ports that acts as a kind of buffer between the external (public Internet) network and your secure network on the other LAN interface. The DMZ gives access to services required from both the external network and the secure network. The services are typically HTTP/FTP (Web) servers for public access, an HTTP/FTP proxy server, an SMTP server and a News (proxy) server. Mail servers and News servers for internal use are placed on the secure network. Through the use of access control list and Firewall, you prohibit access from the Internet to your secure network while still providing access to services on the DMZ.



5. UPnP

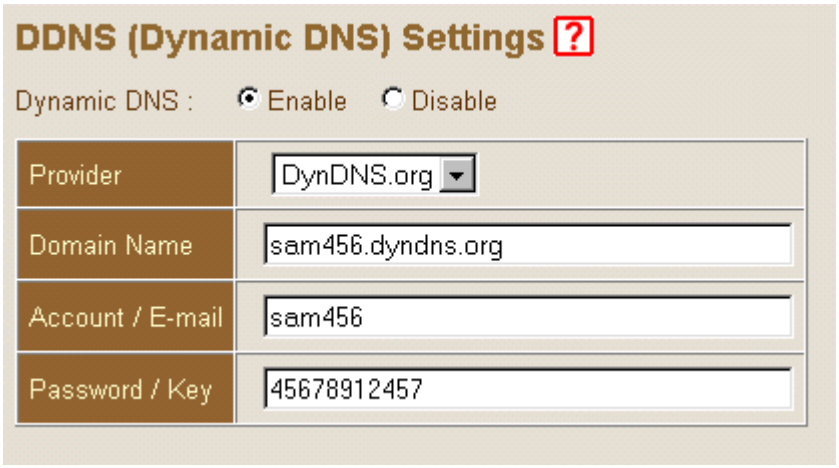
Enable the UPnP can support Windows XP network application. For example, MSN Messenger.



6. Dynamic DNS

Dynamic DNS provides users on the Internet a method to tie their domain name(s) to computers or servers. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes.

We can support two DDNS provider, TZO.com and DynDNS.org. You must apply DDNS service to get Key from DDNS provider and enables the DDNS service.

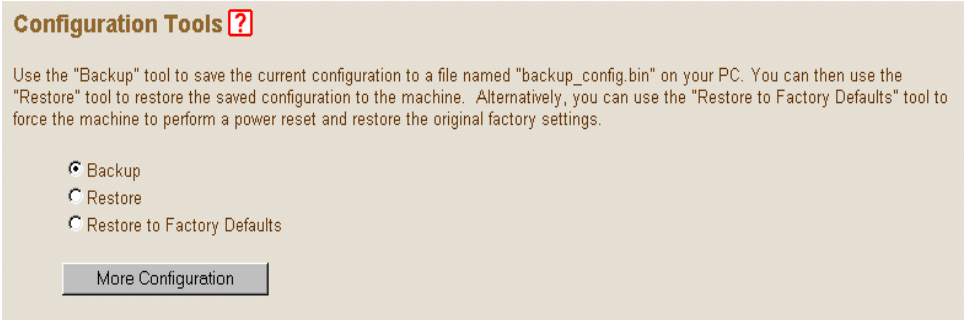


7. Tools

The tools feature provided by VG422R includes configuration tools – save /restore configuration and restore to factory defaults, system log, firmware upgrade and reset. The main page is shown below.

7.1. Configuration Tools

The configuration tools includes backup, restore and restore to factory defaults. The “Backup” tool save the VG422R’s current configuration to a file named “backup_config.exe” on your PC. You can then use “Restore” tool to restore the saved configuration to the VG422R. The “Reset to Factory Deafults” tool will force the configuration of VG422R back to the original factory setting and perform a power reset.

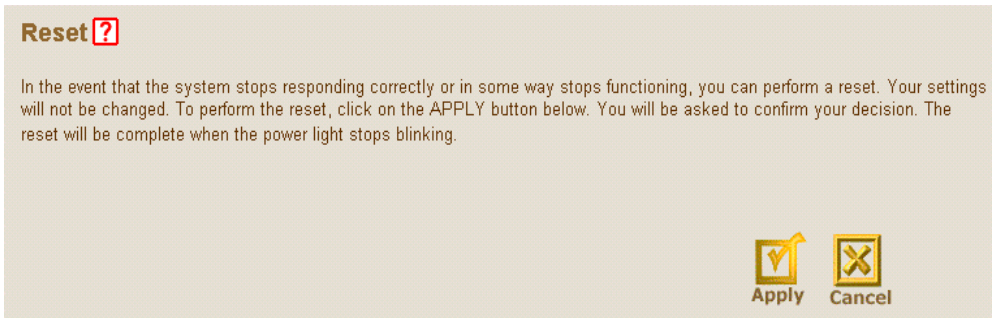


7.2. Firmware Upgrade

The firmware upgrade tool allows you to upgrade the VG422R system firmware. You need to download the file to your local PC first, and select the target to load. The firmware of VG422R is divided into three files, one for core firmware, one for the user interface and one for the voice prompt message.

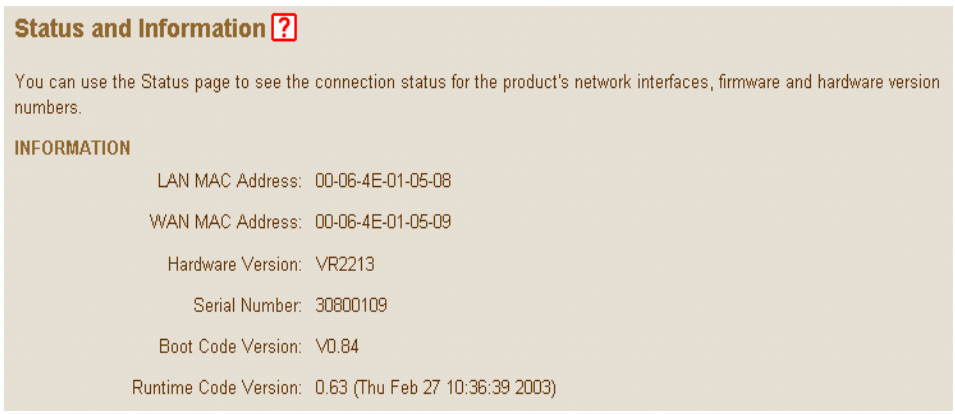
7.3. Reset

In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. Your settings will not be changed. To perform the reset, click on the APPLY button below. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking



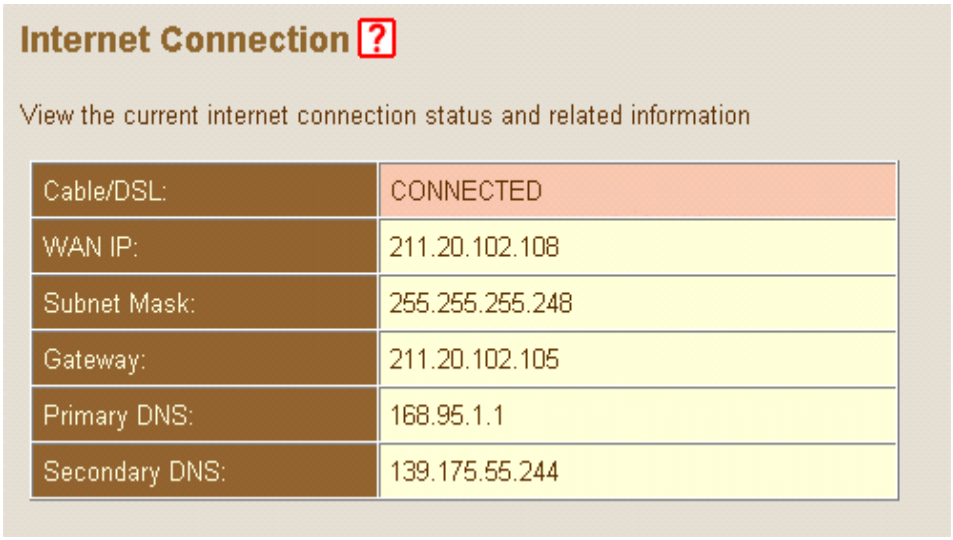
8. Status

The status page displays the status of the system, including the connection status of the interfaces, firmware and hardware version numbers, system log and DHCP client information.



8.1. Internet Connection

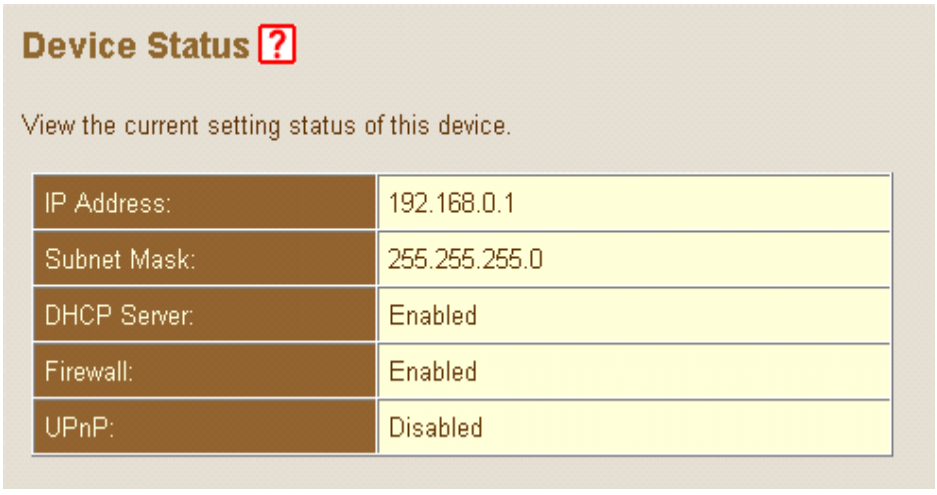
The Internet Connection page displays the status of the Internet Connection, including the connection status of the Internet interfaces, WAN port IP, Subnet Mask, Gateway IP and Primary/ Secondary DNS IP.



When WAN port setting is dynamic IP, user can use <Disconnect> and <Connect> to release and update WAN port IP

8.2. Device Status

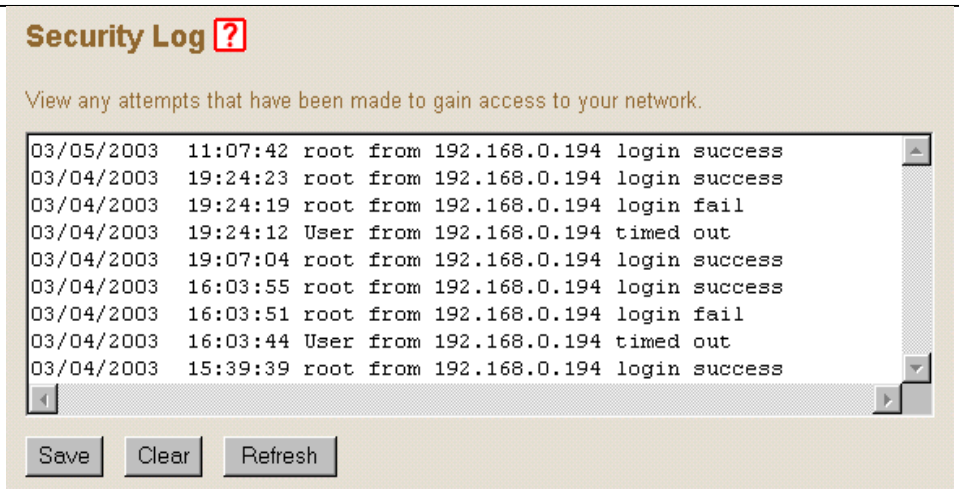
The Device Status page displays the current setting of this device, including IP address, Subnet mask, DHCP server, Firewall and UPnP.



8.3. Security Log

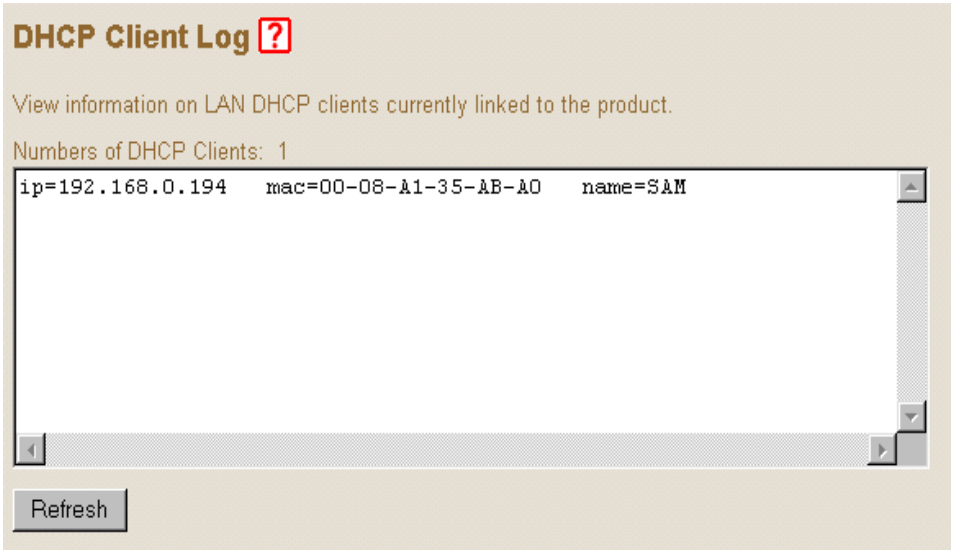
This page provides the system security log recorded when device boot, including user login/logout, hack attach, PPPoE connection, NTP connection, Get IP from DHCP.

These records can be saved to host PC. User also can clear all security records in Security log window and press <Refresh> to update current security records.



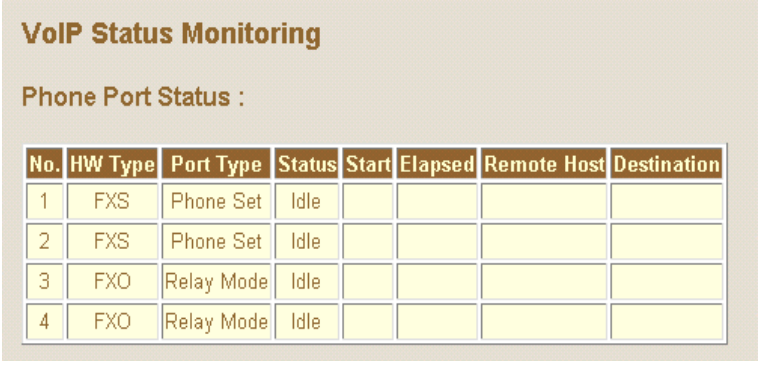
8.4. DHCP Client Log

The DHCP Client Log page displays the IP allocation records. User can press <Refresh> to update current IP allocation records.



8.5. VoIP Status

This page displays the gateway status, including Port Type, Port Status, time information of each call and Destination. This page also displays gatekeeper status. User must make sure gatekeeper registered is OK.



User can press <Refresh> to update current VoIP status.